JAGADISH TRIPATHY

VM Management Specialist | VAPT Practitioner | Penetration Tester | SOC Analyst in Training | Kali Linux & Offensive Security Expert

+917681000901 • jagadishtripathy144@gmail.com • https://www.linkedin.com/in/jagadishtripathy/ • Angul

Summary

Enthusiastic cybersecurity specialist with hands-on experience in penetration testing, cybersecurity tools, and network analysis. Proven ability to develop innovative security strategies and tools, improving threat detection rates significantly. Passionate about tackling system vulnerabilities and enhancing security measures through continuous learning and application of ethical hacking principles. Excited to contribute to cutting-edge security solutions and support the vital mission of safeguarding digital infrastructures.

Key Achievements

Phishing Threat Detection

Improved security posture by detecting 95% of phishing threats.

Security Tool Development

Developed five security tools, increasing threat detection rate by 50%.

Vulnerability Testing

Conducted vulnerability testing on 20 systems, enhancing security by 35%.

Network Analysis Project

Led team to achieve 85% accuracy in network analysis project.

Experience

CODTECH IT SOLUTIONS

Internship Trainee — 09/2024 - 10/2024

Internship

- Penetration Testing: Performed in-depth penetration testing to identify security vulnerabilities in network infrastructures and web applications, simulating real-world cyberattacks to assess risk.
- Vulnerability Analysis: Used industry-standard tools to analyze and report vulnerabilities, recommending and implementing security measures to mitigate risks.
- Network Packet Analysis: Captured and analyzed network traffic to detect potential threats, ensuring systems were secure and protocols adhered to best practices in information security.

YHills

Yhills edutech private limited — 07/2024 - 08/2024

Internship

- Reverse Shell Attacks: Successfully executed reverse shell attacks in controlled environments, simulating potential threats and demonstrating methods for bypassing security mechanisms.
- Technical Reporting: Created detailed technical reports with Proof of Concept (PoC) for each vulnerability found, outlining remediation steps and preventive strategies.
- Ethical Hacking: Applied ethical hacking techniques, using frameworks like Metasploit and tools such as Nmap, to simulate attacks and ensure system integrity while maintaining compliance with ethical standards.

Education

Synergy Institute of Engineering and Technology (SIET), Dhenkanal

Bachelor of Technology - BTech, Computer Science and engineering — 01/2023 - 06/2027

Siddhibinayak Science Higher secondary school Angul

12th — 05/2021 - 04/2023

Government Up Graded High School Nisha

High school — 02/2011 - 03/2021

Certification

Foundations of Cybersecurity — Google

Play It Safe: Manage Security Risks — Google

Certification

Introduction to Networking and Cloud Computing — Microsoft

Tools of the Trade: Linux and SQL — Google

Connect and Protect: Networks and Network Security — Google

Assets, Threats, and Vulnerabilities — Google

Introduction to Computers and Operating Systems and Security — Microsoft

Applied ChatGPT for Cybersecurity — InfoSEC

Projects

Automated Phishing Detection and Response System

10/2024

This project implements an automated system to detect and respond to phishing emails. By integrating email handling, URL analysis using the VirusTotal API, and alert mechanisms, the system identifies suspicious content, quarantines malicious emails, and notifies the security team. The solution enhances cybersecurity measures, streamlining the process of identifying and mitigating phishing threats effectively.

Caesar Cipher Implementation

10/2024 - 10/2024

Caesar Cipher Implementation I developed a Python program to encrypt and decrypt text using the Caesar Cipher algorithm.
#Python #Cybersecurity #Encryption

Image Encryption Tool Using Pixel Manipulation

10/2024 - 10/2024

Image Encryption Tool using Pixel Manipulation A Python-based tool that encrypts images by altering pixel values, rendering them visually blank. The original image can only be restored through decryption, ensuring secure visual obfuscation.

Network Packet Analyzer

10/2024 - 10/2024

Network Packet Analyzer
Developed a Python-based tool to capture and analyze network traffic in real-time, offering insights into source and destination IPs, MAC addresses, protocols (TCP, UDP, ICMP), and payloads. Built using the Scapy library, the tool provides a foundation for understanding network traffic flow and protocol behavior in a controlled environment. This project demonstrates practical skills in network monitoring, protocol analysis, and Python programming.

Purpose: Designed for educational use, promoting ethical practices in network analysis and security research.

Reverse PowerShell Attack on Windows Machine

10/2024 - 10/2024

The process began with the creation of a custom Python payload designed to establish a reverse shell connection back to the attacker's Kali Linux machine. The payload was transferred to the Windows machine via a USB drive and executed through PowerShell, effectively bypassing security measures, including Microsoft Defender. Once the payload was executed, a listener was set up on the Kali machine using Netcat (nc -lvnp 80), allowing the attacker to establish a connection.

The attack successfully provided remote access to the Windows machine, enabling the execution of various commands, such as whoami and dir. This project highlighted the importance of understanding the risks associated with social engineering, endpoint security, and the need for robust defense mechanisms. By documenting the attack and its implications, the project underscores the critical need for organizations to implement effective security measures to mitigate such vulnerabilities and enhance overall cybersecurity resilience.

Projects

Comprehensive Penetration Testing

09/2024 - 09/2024

This project involved a comprehensive penetration test on both a web application and a Windows 7 system to identify and exploit vulnerabilities. For the web application, SQL Injection using sqlmap successfully extracted sensitive data, while SpiderFoot was used for passive reconnaissance, and Nmap for port scanning. The Windows system test focused on exploiting the MS17-010 (EternalBlue) vulnerability using Metasploit, gaining administrative access, and extracting NTLM password hashes, which were then cracked using John the Ripper. This project demonstrated key skills in vulnerability exploitation, password cracking, and penetration testing tools across both web and system environments.

Skills

- Project Management
- Monitoring & Defence
- Network Scanning and Analysis
- System Exploitation and Security Bypass
- Reporting and Documentation